



[DATE]

[NAME]

### NOTICE OF DATA BREACH

Dear [NAME],

I am writing to let you know you that an email account belonging to the National Nurse Practitioner Residency and Fellowship Training Consortium (NNPRFTC) was subject to a phishing attack possibly causing the exposure of some of your personal information. This letter explains what happened, the steps that we are taking in response to the incident, and the resources that we are making available to you. Your trust is most important to us and we take the protection of your information seriously. Therefore, we are offering credit monitoring/identity theft protection services to you at no charge.

### WHAT HAPPENED

NNPRFTC's Executive Director began receiving a high-volume of undeliverable messages on May 25, 2019. Upon further investigation, our IT security team discovered that someone had gained unauthorized access to the email account and set a rule to forward automatically all incoming and outgoing messages. It is unclear exactly when the attacker gained access or whether the attacker used any of the information in the email account. In an abundance of caution, we considered all items in the email inbox to be at risk. Among the thousands of emails in the account, after extensive review, we uncovered only five messages containing sensitive personal information.

### WHAT INFORMATION WAS INVOLVED

We uncovered two emails, dated February 18, 2019 and March 18, 2019, to which was attached a W-2 form and a copy of your driver's license. The attachments contained your name, address, date of birth, and social security number.

### WHAT WE ARE DOING

In addition to our extensive investigation by our IT security and legal teams, we also reported the incident to the Federal Bureau of Investigation's Internet Crimes division. We also implemented additional security measures to the O365 account. To offer you peace of mind, we are offering two years of identity theft monitoring services to all of our clients at no cost. Additionally, we have included information below about additional steps you can take to protect yourself.

### WHAT YOU CAN DO

In addition to enrolling in the identity theft monitoring service detailed below, there are other steps that you can take. Because the information breached may have included your social security number, we encourage you to regularly review your financial accounts and credit reports, and report any suspicious or unrecognized activity immediately. You also may wish to consider placing a fraud alert or security freeze on your accounts. More information about these options is detailed below.

Again, your security and peace of mind are our top priority. We realize you place your trust in us and we never take that trust for granted. Please feel free to contact our Privacy Officer, Tracy Guarnieri, with any questions or concerns at 860-347-6971 x3705.

Sincerely,

Margaret Flinter, APRN, PhD, C-FNP, FAAN, FAANP  
Chair of the Board of Directors

## **Information about Identity Theft Protection**

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

**Equifax:** P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, [www.equifax.com](http://www.equifax.com)  
**Experian:** P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, [www.experian.com](http://www.experian.com)  
**TransUnion:** P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, [www.transunion.com](http://www.transunion.com)

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

**Federal Trade Commission**, Consumer Response Center  
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**For residents of Maryland:** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

**Maryland Office of the Attorney General**, Consumer Protection Division  
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us)

**For residents of Massachusetts:** You also have the right to obtain a police report.

**For residents of North Carolina:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

**North Carolina Attorney General's Office**, Consumer Protection Division  
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, [www.ncdoj.gov](http://www.ncdoj.gov)

**Fraud Alerts:** There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, [www.equifax.com](http://www.equifax.com)  
Experian: 1-888-397-3742, [www.experian.com](http://www.experian.com)  
TransUnion: 1-800-680-7289, [fraud.transunion.com](http://fraud.transunion.com)

**Credit Freezes:** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, <a href="http://www.equifax.com">www.equifax.com</a>
Experian:	P.O. Box 9554, Allen, TX 75013, <a href="http://www.experian.com">www.experian.com</a>
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, <a href="http://freeze.transunion.com">freeze.transunion.com</a>

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

### **Credit Monitoring/Identity Theft Protection Service Information**

#### **What we are doing to protect your information:**

To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: 9/30/19** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [www.experianidworks.com/3bcredit](http://www.experianidworks.com/3bcredit)
- Provide your **activation code:** [CODE]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by 9/30/19. Be prepared to provide engagement number DB12987 as proof of eligibility for the identity restoration services by Experian.

#### **ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:**

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.